IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

BETA TECHNOLOGY, INC.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. H-13-1282
	§	
LEIGH A. MEYERS, SONJA C.	§	
GARCIA, ENCORE INDUSTRIAL	§	
SUPPLY, LLC and ENCORE	§	
INDUSTRIAL PRODUCTS, LLC,	§	
	§	
Defendants.	§	

MEMORANDUM AND ORDER

Pending is Defendants' Motion to Dismiss for Lack of Subject Matter Jurisdiction (Document No. 11). After considering the motion, response, reply, and applicable law, the Court concludes as follows.[1]

I. Background

Beta Technology, Inc. ("Plaintiff") is a specialty chemical company engaged in marketing, promoting, and selling specialty chemicals and related equipment.[2] Defendant Leigh Meyers ("Meyers"), a shareholder in Plaintiff, worked as Plaintiff's

_____

[1] Plaintiff filed its First Amended Complaint, which is currently the live pleading in this case, on the same day that it filed its Response to Defendants' Motion to Dismiss. *See* Document No. 14 (1st Am. Complt.). Defendant's Reply in support of its motion cites Plaintiff's First Amended Complaint. The Court therefore considers Defendants' motion, as the parties have done, as now addressed to the First Amended Complaint.

[2] Document No. 14 ¶ 8.

director and president until he resigned in June 2012.[3] Defendant Sonja Garcia ("Garcia") worked for Plaintiff as an Account Manager until her resignation in December 2012.[4]

When Garcia began her employment with Plaintiff, she entered into an Account Manager Employment Agreement and an Employment Terms and Conditions Agreement ("the Employment Agreements") stating that she would not compete against Plaintiff or solicit its clients in six Texas counties for a two-year period following her separation from the company, and that she would not disclose Plaintiff's confidential or proprietary information.[5] These agreements were signed by Garcia. Meyers, as president of Plaintiff, also signed Garcia's Employment Agreements.[6] Additionally, Plaintiff has an Internet, Intranet, Electronic Mail and Computer Use Policy ("the Computer Use Policy") that it alleges Meyers helped to draft during his employment.[7] The policy provides that it is "inappropriate conduct" to use Plaintiff's computer systems to engage in private or personal business activities, to make unauthorized copies of data, or to delete data.[8]

---

[3] Id. ¶ 9.

[4] Id. ¶ 10.

[5] Id. ¶¶ 11-12.

[6] Id. ¶ 14.

[7] Id. ¶ 15

[8] Id.

Plaintiff alleges that it provided one of its computers to Meyers during his employment, and that "[b]efore or at the time of his resignation," he downloaded Plaintiff's confidential and proprietary information and deleted all stored information from the computer.[9] Plaintiff further alleges that both before and after his resignation, Meyers used this confidential and proprietary information to compete against Plaintiff and solicit its customers and employees.[10]

After ending his employment with Plaintiff, Meyers began working as president and CEO of newly formed competing companies of which he and his wife are alleged to be the sole owners, Defendants Encore Industrial Supply, LLC and Encore Industrial Products, LLC (collectively, "Encore," and together with Meyers and Garcia, "Defendants").[11] Plaintiff alleges that Meyers is working in the same territory in which he previously worked for Plaintiff and that he has solicited several of Plaintiff's customers.[12] Plaintiff further alleges that Meyers solicited Garcia to work for Encore, and that Garcia is currently working in the same territory in which she previously worked for Plaintiff and has solicited business from

---

[9] Id. ¶¶ 17-19.

[10] Id. ¶ 20.

[11] Id. ¶ 21.

[12] Id. ¶ 22.

several of Plaintiff's customers, all in violation of the Employment Agreements.[13]

Plaintiff alleges the following claims: breach of contract against Garcia; breach of fiduciary duty and misappropriation of confidential information and trade secrets against Meyers and Garcia; aiding and abetting breach of fiduciary duty against Encore; tortious interference with business relationships, defamation, and violation of the Texas Deceptive Trade Practices Act against all Defendants; and violation of the Computer Fraud and Abuse Act ("CFAA") against Meyers.[14]   Plaintiff asserts that its CFAA claim provides the Court with subject matter jurisdiction pursuant to 28 U.S.C. § 1331.[15] Defendants move to dismiss for lack of subject matter jurisdiction, contending that Plaintiff has not stated a claim under the CFAA upon which relief can be granted.[16]

II.   Legal Standard

Defendants attack subject matter jurisdiction on the grounds that Plaintiffs fail to state a claim under the CFAA, which is the sole basis for federal jurisdiction over the instant case.[17]   Given

---

[13] Id. ¶ 23.

[14] Document No. 14.

[15] Document No. 15 at 4.

[16] Document No. 11 at 1.

[17] It is uncontroverted that complete diversity is lacking.

4

that Defendants' arguments go principally to the merits of Plaintiffs' CFAA claim, which does not appear to be immaterial or frivolous, the proper disposition of Defendants' motion to dismiss is under Rule 12(b)(6) rather than Rule 12(b)(1). *See* <u>Williamson v. Tucker</u>, 645 F.2d 404, 415 (5th Cir. 1981) ("Where the defendant's challenge to the court's jurisdiction is also a challenge to the existence of a federal cause of action, the proper course of action for the district court (assuming that the plaintiff's federal claim is not immaterial and made solely for the purpose of obtaining federal jurisdiction and is not insubstantial and frivolous) is to find that jurisdiction exists and deal with the objection as a direct attack on the merits of the plaintiff's case."); <u>Herrera v. NBS, INC.</u>, 759 F. Supp. 2d 858, 863 (W.D. Tex. 2010) (finding motion to dismiss for lack of subject matter jurisdiction was really an attack on the merits of the claim, and construing it as a motion to dismiss for failure to state a claim under Rule 12(b)(6)).

Rule 12(b)(6) provides for dismissal of an action for "failure to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). When a district court reviews the sufficiency of a complaint before it receives any evidence either by affidavit or admission, its task is inevitably a limited one. *See* <u>Scheuer v. Rhodes</u>, 94 S. Ct. 1683, 1686 (1974). The issue is not whether the

plaintiff ultimately will prevail, but whether the plaintiff is entitled to offer evidence to support the claims. Id.

In considering a motion to dismiss under Rule 12(b)(6), the district court must construe the allegations in the complaint favorably to the pleader and must accept as true all well-pleaded facts in the complaint. See Lowrey v. Tex. A&M Univ. Sys., 117 F.3d 242, 247 (5th Cir. 1997). To survive dismissal, a complaint must plead "enough facts to state a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 127 S. Ct. 1955, 1974 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 129 S. Ct. 1937, 1949 (2009). While a complaint "does not need detailed factual allegations . . . [the] allegations must be enough to raise a right to relief above the speculative level, on the assumption that all the allegations in the complaint are true (even if doubtful in fact)." Twombly, 127 S. Ct. at 1964-65.

III. Analysis

The CFAA is principally a criminal statute that proscribes various fraudulent and related activities committed in connection with the use of computers. See 18 U.S.C. § 1030. Subsection 1030(g), however, also provides a civil remedy for the recovery of

damages and injunctive relief against one who violates § 1030 and whose conduct involves any factor set forth in subsection 1030(c)(4)(A)(i)(I-V).[18]   Plaintiff alleges that Meyers violated substantive provisions of subsection 1030(a)(4) and (5), and caused loss of more than $5,000 in a one-year period, in violation of subsection 1030(c)(4)(A)(i)(I).[19]

A.   § 1030(a)(4)

       Subsection 1030(a)(4) establishes liability for one who:

       knowingly and with intent to defraud, accesses a
       protected computer without authorization, or exceeds
       authorized access, and by means of such conduct furthers
       the intended fraud and obtains anything of value, unless
       the object of the fraud and the thing obtained consists

---

[18] These are:

(I)   loss to 1 or more persons during any 1-year period . . .
       aggregating at least $5,000 in value;

(II)   the modification or impairment, or potential modification
       or impairment, of the medical examination, diagnosis,
       treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV)   a threat to public health or safety;

(V)   damage affecting a computer used by or for an entity of
       the United States Government in furtherance of the
       administration of justice, national defense, or national
       security . . .

18 U.S.C. § 1030(c)(4)(A)(i)(I-V).

[19] Document No. 14 ¶¶ 51-55.

only of the use of the computer and the value of such use
is not more than $5,000 in any 1-year period;

18 U.S.C. § 1030(a)(4).   The CFAA defines "exceeds authorized
access" as meaning "to access a computer with authorization and to
use such access to obtain or alter information in the computer that
the accesser is not entitled so to obtain or alter." Id.
§ 1030(e)(6).

Defendants contend that Meyers's computer was provided to him
by Plaintiff, and thus he did not access the files on it "without
authorization."[20]   Defendants also argue that Meyers's subsequent
misuse of Plaintiff's confidential information did not "exceed[]
authorized access."[21]

Plaintiff has adequately alleged that Meyers exceeded his
authorization to access the computer.   The Fifth Circuit has
recognized that "[a]ccess to a computer and data that can be
obtained from that access may be exceeded if the purposes for which
access has been given are exceeded." United States v. John, 597
F.3d 263, 272 (5th Cir. 2010).   In John, the defendant was an
account manager at Citigroup who was authorized to access customer
account information. Id. at 269.   She accessed and printed
information related to seventy-six customer accounts and provided
it to her half-brother, who used the information to incur

---

[20] Document No. 11 at 5.

[21] Id..

fraudulent charges. Id. The defendant was criminally convicted under the CFAA, but appealed her conviction on the grounds that the CFAA does not prohibit the unlawful *use* of materials that she was permitted to access. Id. at 271. The Fifth Circuit found that the defendant exceeded her authority to access Citigroup's information, because her authority to access the information was limited by Citigroup's official policy, which prohibited misuse of confidential customer information. Id. at 272.[22]

Like the defendant in John, Meyers's authorization to use Plaintiff's computer system and the data contained therein was circumscribed by company policy. Plaintiff alleges that Meyers himself helped draft the Computer Use Policy adopted by Plaintiff, which defined "inappropriate conduct" to include:

---

[22] In John, the Fifth Circuit observed that merely violating an employer's confidentiality agreement may not be sufficient to constitute a violation of the CFAA. 597 F.3d at 272. However, Meyers did not just violate a confidentiality agreement, he also violated the Computer Use Policy, which explicitly prohibited making unauthorized copies of company data. Defendants cite to two Southern District of Texas cases in support of the proposition that misuse of information that one is authorized to access does not qualify as exceeding that authorization. However, both cases predate the Fifth Circuit's ruling in John. *See* Joe N. Pratt Ins. v. Doane, Civ. A. No. V-07-07, 2009 WL 3157337, at *2 (S.D. Tex. Sept. 25, 2009) ("Pratt's complaint is that Doane and Turner *misused* the business information they gathered from Pratt's system, which they were undoubtedly authorized to access. The Court concludes that such a theory cannot support a claim under the CFAA."); Bridal Expo, Inc. v. van Florestein, Civ. A. No. 4:08-cv-0377, 2009 WL 255862, at *10 (S.D. Tex. Feb. 3, 2009) (declining to find that an employee exceeds her authorization under the CFAA when she has authorization to access the files but later uses them to harm the employer).

- Engaging in private or personal business activities, including use of instant messaging and chat rooms;

- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access;

- Making unauthorized copies of Company files or other Company data;

- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company.[23]

Plaintiff alleges that Meyers violated this policy by making unauthorized copies of Plaintiff's confidential information and then deleting stored information from the computer.[24] Furthermore, Meyers allegedly did so to compete against Plaintiff and to solicit Plaintiff's customers, violating the policy's prohibition against using Plaintiff's computer system for his own 'private or personal business activities.'[25] Accordingly, Plaintiff's allegations are that Meyers's actions exceeded his authorized access. *See* Meats by Linz, Inc. v. Dear, Civ. A. No. 3:10-CV-1511-D, 2011 WL 1515028, at *3 (N.D. Tex. April 20, 2011) (Fitzwater, J.) (holding plaintiff stated a claim under the CFAA where it alleged facts allowing the court to draw the reasonable inference that defendant accessed plaintiff's computer system and data and used it, in violation of

---

[23] Document No. 14 ¶ 15.

[24] Id. ¶¶ 17-19.

[25] Id. ¶ 20.

the restrictive covenant agreement, to compete directly with plaintiff and solicit its customers) (citing <u>John</u>, 597 F.3d at 271-72).

Defendants further contend that Plaintiff has failed to state a claim under subsection (a)(4) because he did not "obtain[] anything of value" when he deleted data from the computer. 18 U.S.C. § 1030(a)(4).[26] However, Plaintiff's First Amended Complaint alleges that Meyers downloaded "confidential and proprietary information" before deleting the files,[27] which sufficiently alleges that he obtained something of value. Accordingly, Plaintiff has stated a claim under subsection (a)(4) of the CFAA.

B.   § 1030(a)(5)

Subsection 1030(a)(5) establishes liability for anyone who:

(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

---

[26] Document No. 11 at 7.

[27] Document No. 14 ¶ 19.

18 U.S.C. § 1030(a)(5). Plaintiff asserts violations by tracking
the proscriptive language of subsection 1030(a)(5)(A) and (C).[28]

Plaintiff has successfully stated a claim under subsection
1030(a)(5)(A). This subsection forbids damaging computers without
authorization. <u>Hewlett-Packard Co. v. Byd:Sign, Inc.</u>, No. 6:05-CV-
456, 2007 WL 275476, at *13 (E.D. Tex. Jan. 25, 2007).[29] Subsection
1030(e)(8) defines "damage" as "any impairment to the integrity or
availability of data, a program, a system, or information."
Plaintiff has alleged that Meyers was not authorized to delete
company data, and yet installed and used the ARO 2012 computer
program in an attempt "to permanently delete all of [Plaintiff's]
information from the computer."[30]   Accordingly, Plaintiff has
stated a claim that Meyers violated subsection 1030(a)(5)(A). *See*
<u>Hewlett-Packard</u>, 2007 WL 275476 at *13 (denying motion to dismiss
subsection 1030(a)(5)(A) claim where employees were not authorized
to damage plaintiff's computers by 'scrubbing' data).

Plaintiff has also stated a claim under subsection
1030(a)(5)(C).   Plaintiff alleges that Meyers "knowingly and
intentionally accessed [Plaintiff's] protected computer system
without authorization, causing damage and loss,"[31] which is the

---

[28] Document No. 14 ¶ 54.

[29] <u>Hewlett-Packard</u> cites an earlier, but substantively
identical, provision of the CFAA. 2007 WL 275476 at *12-13.

[30] Document No. 14 ¶¶ 15, 18.

[31] <u>Id.</u> ¶ 54.

proscription of the statute, and that "[b]efore or at the time of his resignation" Meyers "deleted all the stored information from the computer."[32]   Reading the First Amended Complaint in the light most favorable to Plaintiff raises an inference that Meyers may have accessed the computer at the time of his resignation after he was no longer employed by Plaintiff, and thereby accessed the computer without authorization.[33]

C.   § 1030(c)(4)(A)(i)(I)

Plaintiff alleges that Meyers can be held civilly liable for his violations of the CFAA because he caused loss of more than $5,000 in a one-year period, in violation of subsection

---

[32] Id. ¶17.

[33] Moreover, it has been held that one who breaches his duty of loyalty to his employer cannot rely on the cloak of authority. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) ("Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop."). See also U.S. v. Phillips, 477 F.3d 215, 221 & n.5 (5th Cir. 2007) ("[C]ourts have recognized that authorized access typically arises only out of a contractual or agency relation- ship.") (citing Citrin, 440 F.3d 418).   Plaintiff's allegations permit an inference that even before Meyers resigned his employment, he had surreptitiously acted in breach of his duty of loyalty to Plaintiff such as to cause the termination of his agency relationship with Plaintiff along with all corresponding authority he previously had enjoyed to access Plaintiff's protected computer system.   But see United States v. Nosal, 676 F.3d 854, 862 (9th Cir. 2012) (rejecting Citrin's holding that the CFAA covers violations of the duty of loyalty); WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012)("[W]e reject any interpretation that grounds CFAA liability on a cessation-of-agency theory.").

1030(c)(4)(A)(i)(I).   *See* 18 U.S.C. § 1030(g).   Plaintiff's First Amended Complaint states that Plaintiff "incurred, and continues to incur, significant expenses in assessing and recovering the data deleted from the computer," and that this has resulted in a loss of more than $5,000 in any one-year period.[34]   Accordingly, Plaintiff has stated a claim that Meyers violated subsection 1030(c)(4)(A)(i)(I), and can be held civilly liable under the CFAA.

IV. Order

Accordingly, it is

ORDERED that Defendants Leigh A. Meyers, Sonja C. Garcia, Encore Industrial Supply, LLC, and Encore Industrial Products, LLC's Motion to Dismiss for Lack of Subject Matter Jurisdiction (Document No. 11) is DENIED.   The Clerk will enter this Order, providing a correct copy to all counsel of record.

SIGNED in Houston, Texas, this 10TH day of October, 2013.

EWING WERLEIN, JR.
UNITED STATES DISTRICT JUDGE

---

[34] Id. ¶ 53.